Security Architecture and Design Documentation Guidance

SECURITY OBJECTIVES

Version 2.2

Prepared by HR CDS TT

3 March 2011

REVISION HISTORY

Name	Date	Reason For Changes	Version
HRCDSTT	7 Oct 2010	Document creation	1.0
HRCDSTT	20 Oct 2010	Tiger Team review and update	2.0
HRCDSTT	21 Oct 2010	Tiger Team review and update	2.1
HRCDSTT	3 Mar 2011	Tiger Team review and update	2.2

ACRONYMS AND DEFINITIONS

Acronym	Definition
CCA	Covert Channel Analysis
CDS	Cross Domain Solution
DRD	Data Representation Documentation
DTLS	Descriptive Top-Level Specification
FTLS	Formal Top-Level Specification
HLD	High Level Design
LLD	Low Level Design
SP	Security Policy

INTRODUCTION

Security objectives are a list of statements that express the intent to satisfy the identified security problem that, when implemented in concert with the assumptions, are able to counter anticipated threats.

The security objectives are derived from the security problem. The security policy is a more detailed traslation of the security objectives into a consise set of rules. The security objectives in conjunction with the security policy are used to derive the security requirements. See Figure 1.

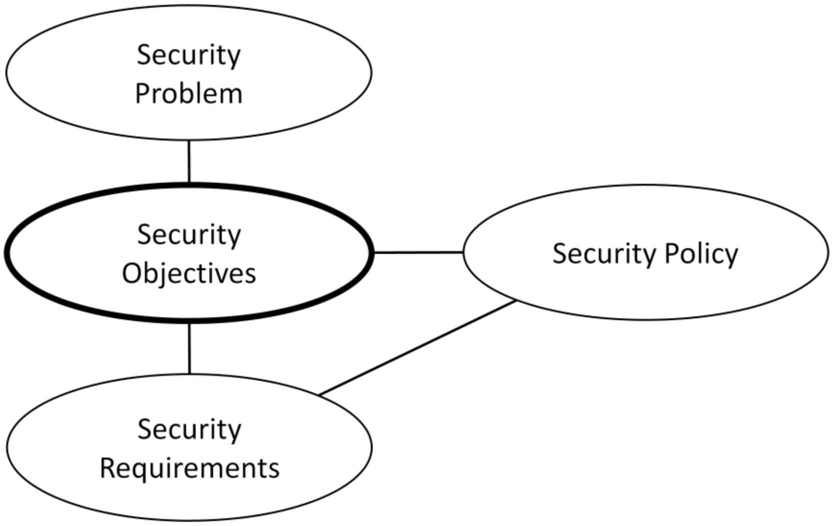

Figure 1 - Security Objective Interactions

SECURITY OBJECTIVES

Security objectives should be stated in terms of what needs to be accomplished (i.e., performance objectives) not how it is to be accomplished.

The following are abstract security objectives for Cross Domain Solutions:

End of Life (EOL) secure disposition: Sensitive data resident on the solution is protected from disclosure upon solution release and disposal.

Evidence necessary to reconstruct activities on system: Ability to collect, retain, and analyze evidence necessary to reconstruct activities on system (e.g., in case of failure, to be able to identify a failure, to identify the cause of failure, to identify the extent of mission damage, and attempts to circumvent security policy).

Establish, maintain, and recover to secure state: The secure state required for the correct implementation of the security functionality of the system.

Management Administration: Solution security parameters are configurable by privileged users. Users and administrations are adequately educated, trained, and informed on the proper configuration, management, and operation of the solution.

Only security policy authorized access/information flows: Solution functions implement necessary protections to ensure complete, accurate enforcement of the security policy.

Resource availability: Solution resources are fault tolerant, priority constrained, and allocated in such a manner to ensure availability.

Self protection: Security functions and their data of the solution are protected from unauthorized modification.

Sufficient assurance for mission accomplishment: The level of assurance provides the confidence that the mission objectives with be accomplished.

THREATS

Threats are constantly changing. CNSSI No. 4009 defines threat as:

> *"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service."*

The threats are in fact another level of assumptions. Threats are potential events, which may result in violation of the solution's security policy or exercise a lack of comprehensiveness[1] in the solution's security policy. The evaluator(s) should validate that the solution behaves according these assumptions.

The solution should be capable of addressing the known threats, as well as provide best possible protection against anticipated threats. Appendix A provides a characterization of some of the possible threats to the solution.

[1] A threat that exercises a lack of comprehensiveness in the solution's security policy is exploiting an aspect that was not described by the solution's security policy.

APPENDIX A

THREATS

Access to Security-Relevant Data

Security-relevant[2] data is read, modified, or deleted without the necessary authorization when the data is stored or transmitted.

Access to User Data

User data is read, modified, or deleted without the necessary authorization when the data is stored or transmitted.

Administrative Error

Administrators incorrectly install or configure an information system, resulting in ineffective security mechanisms.

Altered Delivery

An information system is corrupted or otherwise modified during delivery such that the on-site version does not match the legitimate version.

Evaluation and Test

There is a lack of or insufficient evaluation and testing to demonstrate that all security mechanisms operate correctly, are nonbypassible, are always invoked and are tamperproof, resulting in the failure to discover inconsistent and/or incorrect behavior.

Implementation Errors

Unintentional or intentional errors occur in the implementation of the design, leading to exploitable flaws.

Insecure State

A system crash, security service disruption, security mechanism failure, or improper initialization, places the information system in an insecure state.

[2] Any data/event that is related to the correct operation and enforcement of the security policy(ies).